フォーク達
ネットワークを変わる

Thaddeus Dryja
BC-2 2017-08-01

intro

- ビットコインはソフトウェアのルール、みんなのパソコンが同意する
- でも、そのルール、どうやって同意する？

ビットコインとForks

- 分かりにくいトピック
- 今日と関係有るトピック！（８月１日）
- ブロックの戦争
- 言葉でもみんな同意してない

ノードの階層

- fullノード
  - 全てのブロック確かめた、utxoセットあり
- Prunedフールノード
  - fullだけど、ブロック歴史を消した
- SPVノード
  - Utxoセット無し PoWで正しさを計る

ルール

- Header
  - PoW, time, 難しさ
- ブロックのルール
  - 大きさ, merkle root, 手数料
- 取引のルール
  - LockTime, 残高, version
- Inputのルール
  - nSequence, signatures

フォークの２種類

- Soft
  - ルールを厳しくする
- Hard
  - ルールを優しくする

    (“hard” なのに）

フォークの２種類

- Soft
  - ルールを厳しくする
- Hard
  - ルールを優しくする

    (“hard” なのに）

フォークの例え

- Soft
  - z文字が入ってるアドレスは禁止
- Hard
  - 署名が1ビット間違ったらドンマイ

soft

- z文字が入ってるアドレスは禁止

- 前のソフト、何でものアドレス大丈夫
- 変わったソフト、z入ってるアドレスが駄目
- 前のソフトが新しいルール気づかないかも
- 新しいソフトは気づく

hard

- 署名が1ビット間違ったらドンマイ
-
- 前のソフト、署名厳しく確認
- 新しいソフト、ちょっと間違ったら許す
- 新しいソフト、前のブロックも大丈夫
- 前のソフト、新しい適当ブロックは断る

ハッシュパワー

- 0%　から　50%
- 50%
- 51%　から　100%

Fork chart

	Hash Power 0%	50%	100%	
Soft	古: 変化無 新: 停止	古:変化無 新:ルール増す 2つに分かれる	古:ルール増す 新:ルール増す 分かれない	古: 増す 新: 増す 分かれない
Hard	古: 変化無 新: 変化無	古:変化無 新:変化無 分かれない	古:変化無 新:ルール減る 2つに分かれる	古: 停止 新: 減る

Fork chart - ABC

Hash Power

Soft + Hard full fork reciprocal	0%	50%	100%	
	古: 変化無 新: 停止	古: 変化無 新: ルール変わる 2つに分かれ	古: 変化無 新: ルール変わる 分2つに分かれ	古: 停止 新: 変わる 分かれる

Replay

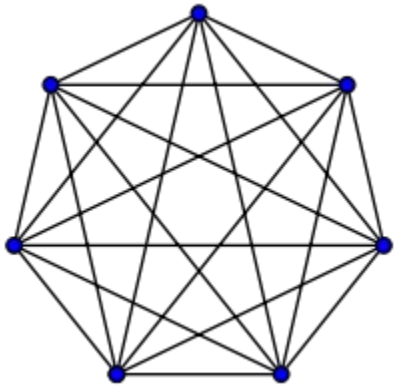
- ２つに分かれたネットワークには同じutxo
- 新しいブロックチェーンの取引は前のネットワークにコピー出来ます
- 取引又は署名の形を変わったら、replay出来ません

2つの「ビットコイン」

- 今まで分かれてない
- 今日2つに分かれる？
- Clamsというコイン、utxo snapshot
- 他のaltcoinも
- 取引所が喜ぶ（手数料いっぱい貰う）

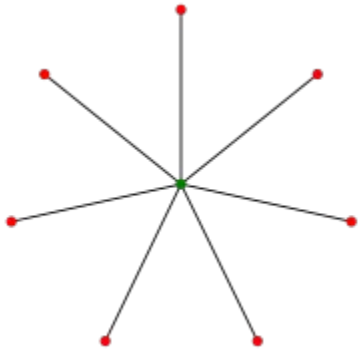
お金の scalability と centralization

お金がない



$O(n^2)$

お金



$O(n)$

2つの「ビットコイン」

- Fork等 altcoin等　いっぱいあれば、お金の意味がなくなる
- 私見ですが、分かれないのは大切。欲しいforkが出来なくても、一つのネットワークを守ります。
- しかし、自由のシステムです。ある人が別のネットワークを作りたければ、　自由に出来ます。

2つの「ビットコイン」

- Fork等 altcoin等　いっぱいあれば、お金の意味がなくなる
- 私見ですが、分かれないのは大切。欲しいforkが出来なくても、一つのネットワークを守ります。
- しかし、自由のシステムです。ある人が別のネットワークを作りたければ、　自由に出来ます。
- 終了 - 質問お願いします！